

## CYBERSECURITY FACTSHEET

### QUICK INDUSTRY SURVEY: SMEs

Prepared by Jacqueline Ferrari, M.A.

## Statistics and Facts on Cyber-Attacks and Privacy Breaches

- The Ponemon Institute calculated that SMEs and smaller businesses are hit proportionately harder than large businesses. The **costs to SMEs** are estimated to range from hundreds of thousands of dollars to **US\$20m per organization** (Baker Tilly International, 2016).
- A report from PwC found that **74 percent of SMEs** reported a security breach. However, **only 7 percent of small businesses expect information security spending to increase** in the next year (Sampson Hall, 2016).
- According to the National Cybersecurity Alliance, **1 in 5 small businesses** fall victim to cybercrime each year. And of those, **60 percent go out of business within six months** after an attack (Optimal Networks, 2016; Marquez, 2016).
- **Over 77 percent** of all cybercrimes target SMEs and yet, research shows **42 percent of SMEs don't see cybercrime as a risk** (FireEye, 2016).
- According to a Kaspersky Lab survey, **small businesses shell out an average of \$38,000 to recover from a single data breach** (Conlan, 2015).
- According to Ponemon Institute, **incident response plans, the extensive use of encryption, CISO leadership, employee training and insurance protection can help reduce the costs of a data breach** (Conlan, 2015).
- **Only 31 percent of small businesses take active measures to guard themselves** against security breaches. Furthermore, **41 percent of small businesses are unaware** of the risks accrued with human error, and only **22 percent of small businesses are willing to improve security measures** from last year (Marquez, 2016).
- More than **50 percent of SMEs have been breached in the last 12 months**. The most **prevalent attacks against smaller business are web-based and involve phishing and social engineering breaches** (Keeper Security, 2016).
- **35 percent of SMEs** say the company "owner" manages IT security (Eset, 2016).
- **More than 40 percent** of small businesses said they **don't provide any cybersecurity training or education for employees** (Eset, 2016).

## The State of Cybersecurity in SMEs

No business is too small to evade a cyber-attack or data breach. Ponemon Institute released their *2016 State of Cybersecurity in Small and Medium-Sized Business* report. The report contains 10 key findings that reveal the state of cybersecurity in SMEs. These findings include:

1. The most predominant attacks against SMEs are web-based and phishing/social engineering.
2. Negligent employees or contractors and third parties caused most data breaches. However, the root cause of the breach could not be determined in almost one-third of companies.
3. Businesses are most concerned about the loss of theft to their customer's information and their intellectual property.
4. Strong passwords and biometrics are believed to be a crucial component to security protection.
5. Password policies are not strictly enforced. Additionally, policies do not require employees to use a password or biometric to secure access to mobile devices.
6. Current technologies cannot identify and prevent many cyber-attacks. Most breaches have evaded intrusion detection systems and anti-virus solutions.
7. Personnel, budget, and technologies are insufficient to have a strong security posture.
8. Determination of IT security priorities is not consolidated.
9. Web and intranet servers are considered the most vulnerable endpoints or entry points to networks and enterprise systems.
10. Mobile devices and cloud usage that access business-critical applications and IT infrastructure will increasingly threaten the security posture of businesses.

## Best Practices for SMEs to Prevent Cyber-Attacks<sup>1</sup>

**Malware Protection:** Install anti-virus solutions on all systems and keep your software and web browsers up-to-date. Restrict access to inappropriate websites to lessen the risk of being exposed to malware.

**Network Security:** Increase protection of your networks, including wireless networks against external attacks through the use of firewalls, proxies, access lists and other measures.

**Secure Configuration:** Maintain an accurate account of all IT equipment and software. Identify a secure standard configuration for all existing and future IT equipment used by your business.

**Encrypt Your Data:** Encode personal and sensitive information both in transit and at rest. Regularly review who has access to what data and revoke access for those who no longer require it.

**Strong Authentication:** Use two-factor authentication for added privacy and safety.

---

<sup>1</sup> Best practices were taken from a number of sources including: HM Government, 2015; Insight Consultants, 2015; Sampson Hall, 2016; and Taylor, 2016.

(U.S.) Main Office & Mailing Address: 347 Fifth Avenue, Suite 1402-285. New York, New York, 10016, USA

(U.S.) 2<sup>nd</sup> Office Location: 326 Broad Street, Utica, New York 13501, USA

(Canada) Mailing Address: PO BOX # 47056. 2638 Innes Road. Ottawa, Ontario. K1B5P9 CANADA

(Canada) Office Address: 255 Centrum Blvd., Suite 102, Ottawa, ON, K1E 3W3 CANADA

T: 646-205-2246 T2: 613-286-6484 URL: [www.XAHIVE.com](http://www.XAHIVE.com), Email: [sem@xahive.com](mailto:sem@xahive.com)

**Generate Stronger Passwords:** If two factor authentication isn't feasible or available, users must be made to create diverse passwords that combine numbers, symbols, and other factors to ensure safety and security. Passwords should be updated frequently.

**Educate Employees:** Ensure employees are aware of cyber security threats and how to deal with them. Keep employees informed about appropriate handling and protection of sensitive data. In addition, each business should provide cybersecurity training sessions and courses tailored to business needs.

**Delete Suspicious Emails:** Delete suspicious emails as they may contain fraudulent request for information or links or viruses. Unsolicited emails often contain attachments or hyperlinks.

**Monitor Administrative Privileges:** Avoid using an account with administrative privileges for normal day-to-day activities and web browsing.

**Monitor Access:** Restrictions should be implemented on accessing personal information to avoid the potential for a cyber-attack. Each business should monitor access to their network, including memory sticks and other plug-in devices, which can be used to steal company information.

**Deploy Incident Management Plan:** Develop an incident response and disaster recovery capability. Incident management plans must be established and tested. Training must be provided to an incident management team and criminal incidents should be reported to law enforcement.

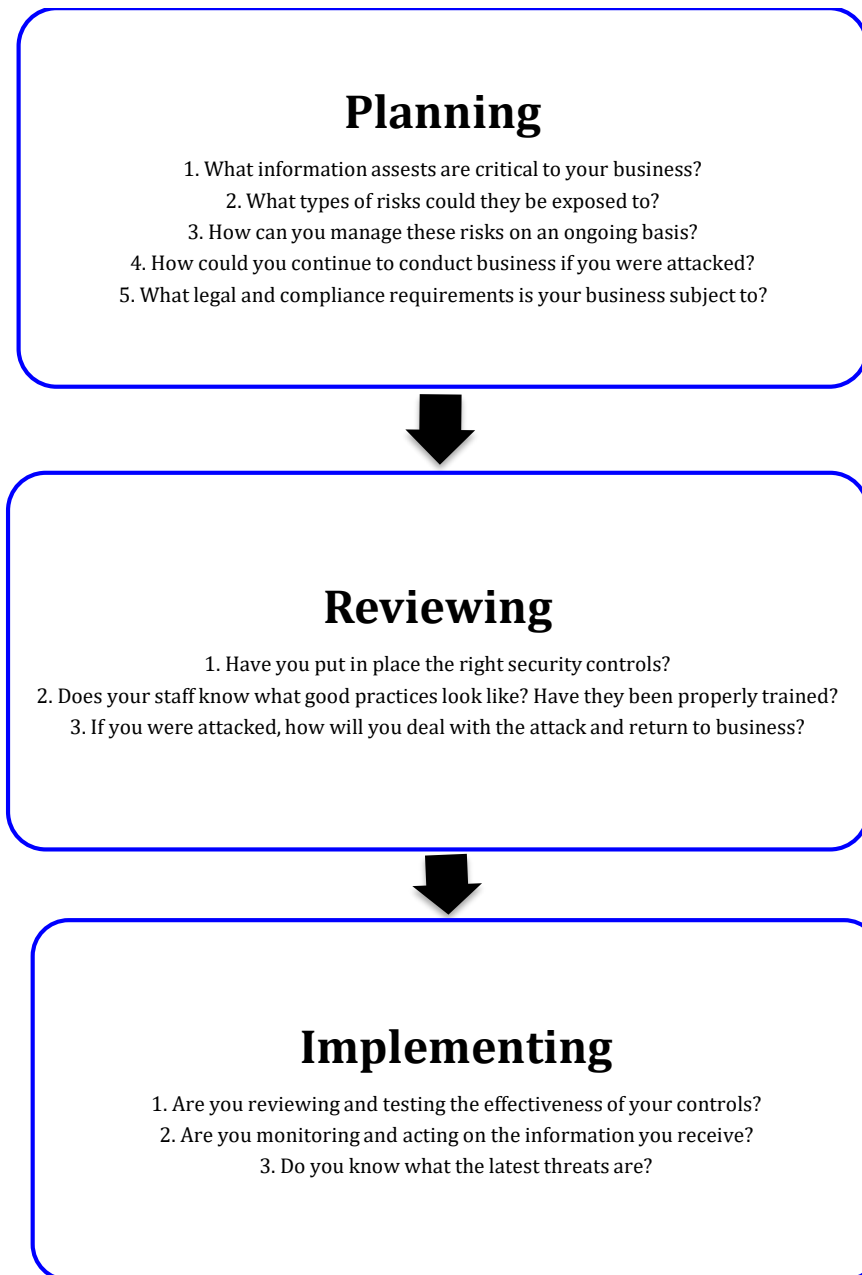
**Internal Governance:** Understand where your information is and who has access to it. Identify a team with security expertise and designate decision-making authority to the team in the event that a cyber-attack takes place.

**Insurance Protection:** Get an insurance policy that covers any losses from cybercrime.

## How SMEs Can Manage Cyber Risks

Taking some simple actions and practising safe behaviours will reduce the risk of cyber-attacks. The figure below illustrates how SMEs can manage cyber-attacks and questions to consider (HM Government, 2015).

**Figure 1. Managing Cyber Risks**





Your Cybersecurity Partner

## References

- Baker Tilly International. (2016). *SMEs in the Front Line to Combat Cybercrime*. Retrieved from Baker Tilly International: <http://www.bakertillyinternational.com/web/insights/smes-in-the-front-line-to-combat-cybercrime.aspx>
- Conlan, Meg. (2015, October 20). *Cost of Data Breaches High for Small Businesses*. Retrieved from BizTech: <https://www.biztechmagazine.com/article/2015/10/data-breach-costs-are-high-small-businesses>
- Eset. (2016, May 3). *4 Stats That Will Make You Rethink Cybersecurity for Your Small Business*. Retrieved from Eset: <https://www.eset.com/us/resources/detail/4-stats-that-will-make-you-rethink-cybersecurity-for-your-small-business/>
- FireEye. (2016). *Small and Midsized Businesses: Simple, affordable cyber security solution for your growing enterprise*. Retrieved from FireEye: <https://www.fireeye.com/solutions/small-and-midsize-business.html>
- HM Government (2015, March). *Small businesses: What you need to know about cyber security*. Retrieved from Cyberstreetwise: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf)
- Insight Consultants (2015). *Top 5 Tips for SMEs to prevent Cyber attack*. Retrieved from Insight Consultants: <http://www.insightconsultants.co/down-to-earth-ideation/tips-prevent-cyber-attack-sme/>
- Keeper Security (2016, June 30). *Keeper and Ponemon Institute Study Finds More Than 50% of SMBs Breached in Past Year*. Retrieved from Marketwired: <http://www.marketwired.com/press-release/keeper-and-ponemon-institute-study-finds-more-than-50-of-smbs-breached-in-past-year-2138885.htm>
- Marquez, Oscar. (2016, July 26). *The Costs and Risks of a Security Breach for Small Businesses*. Retrieved from Security: <http://www.securitymagazine.com/articles/87288-the-costs-and-risks-of-a-security-breach-for-small-businesses>
- Optimal Networks. (2016). *What are the Top Cybersecurity Threats to SMBs?* Retrieved from Optimal Networks: <http://www.optimalnetworks.com/top-cybersecurity-threats-small-medium-businesses/>
- Ponemon Institute. (2016, June). *2016 State of Cyber Security in Small and Medium-Sized Businesses (SMB)*. Retrieved from Ponemon Institute: <https://signup.keepersecurity.com/state-of-smb-cybersecurity-report/>
- Sampson Hall. (2016). *5 steps for SMEs to help prevent cyber attacks*. Retrieved from: <http://www.sampsonhall.co.uk/why-smes-shouldnt-be-putting-cyber-security-on-the-back-burner/>
- Taylor, Andy. (2016, July 26). *SMEs still not doing enough to protect themselves from cyber attacks*. Retrieved from APMG International: <http://www.smeweb.com/sme/smes-still-not-doing-enough-to-protect-themselves-from-cyber-attacks>